

ABSTRACT OF THE DISCLOSURE

Provided is an IC card (10) having an EEPROM (104) for storing secret keys for a plurality of 5 digital signatures, and a coprocessor (106) for generating a digital signature using any one of the plurality of secret keys. If a key change command has been received, the secret key used by the IC card (10) is changed to a secret key specified by the key change 10 command. As a result, a secret key for a digital signature that is different from that of a general user can be provided to a special user without raising the cost of manufacturing the IC card.